REMARKS

Amendments to the Claims

Claim 1 was amended to remove the words "application in a wireless transceiver" from the preamble, add the word "comprising" to the preamble, remove the word "desired," replace the word "the" with the word "a" to establish an antecedent basis for the wireless transceiver, add the words "a firewall application in," and replace the words "another" with the words "second" to refer to a second wireless transceiver.

Claim 6 was amended to add the word "a" to correct a grammatical error.

Claims 13 and 26 were amended to replace the words "scanning" with the words "cracking."

Claim 27 was amended to remove the words "application in a base station" from the preamble, replace the words "desired" with the words "first" and "second," replace the word "the" with the word "a" to establish an antecedent basis for the base station, and replace the word "a" with the word "the" to use the established antecedent for the base station.

Claim 29 was amended to remove the words "application in a wireless transceiver" from the preamble, remove the word "desired," replace the word "the" with the word "a" to establish an antecedent basis for the wireless transceiver, and add the words "a firewall application" and replace the "another" with the words "second" to refer to a second wireless transceiver.

Claim 30 was amended to remove the words "application in a wireless transceiver" from the preamble, remove the word "desired," replace the word "the" with the word "a" to establish an antecedent basis for a wireless transceiver, add the words "a firewall in" and replace the words "another" with the words "second" to refer to a second wireless transceiver.

Claim 31 was amended to remove the word "desired,"add the words "a firewall in" and replace the words "another" with the words "second" to refer to a second wireless transceiver.

Claim 32 was canceled without prejudice.

Objections to the Specification

At paragraph 2 of the Office Action, the disclosure was objected to because of an informality.

In the paragraph starting on page 7, line 26 the wording "32a" was changed to "16a" to make the written specification conform to the originally filed drawings. Applicant believes this change overcomes the objection to the specification and respectfully requests that the objection be withdrawn.

Claim Objections

At paragraph 3 of the Office Action, the Examiner objected to the word "another" used in claim 1 at line 10. Applicant has amended claim 1 to use the words "second wireless transceiver" to refer to the previously presented "another wireless transceiver." Applicant believes this change overcomes the above objection to claim 1 and respectfully requests that the objection be withdrawn.

§ 112 Rejections

At paragraph 4 of the Office Action, claims 1-13, 16, 17, 22, 26 and 31 were rejected under 35 U.S.C. § 112 as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

In the Office Action, the Examiner has rejected claims 1, 2-13 and 31 noting that the term "desired" is subjective.

Applicant has amended claims 1 and 31 to remove the word "desired" from the claims. Applicant respectfully requests that the above rejection to claims 1, 2-13 and 31 be withdrawn.

In the Office Action, the Examiner rejected claims 4, 5, 16 and 17 noting that the claims and specification do not provide a standard for ascertaining the term "Base Station Processor (BSP)."

Applicant respectfully submits that BSPs are well described in the specification to enable one of ordinary skill in the art to ascertain a standard for the term BSP. Specifically, Applicant respectfully directs the Examiner's attention to the description of a BSP in Figs. 1, 2, 3 and 5 as originally filed as well as the corresponding text at page 2, lines 3-8 and lines 23-26, page 3, lines 24-26, page 5, line 25 to page 6, line 4, and page 7, line 26 to page 8, line 9 of the originally filed specification. BSPs are clearly illustrated and described by the Applicant as a unit that interfaces subscriber access units with a network, such as the Internet. Further, the BSPs are described as

performing many functions, such as supporting many subscriber access units (see page 2, lines 23-26), providing mobile user login capabilities (see page 3, lines 24-26), providing transceiver capabilities to communicate with the subscriber units (see page 5, line 25 to page 6, line 4) and is involved in the hand-offs of wireless units (see page 7, line 26 to page 8, line 9, and Fig. 3). These functions as well as other functions of BSPs described in the specification are related to functions performed by Base Station Controllers (BSCs) which are well known in the art of wireless communication. Applicant, thus, respectfully submits that a person skilled in the art of wireless communication should be able to ascertain a standard for the term BSP from what is known in the art as well as from the above-noted particular descriptions and other descriptions of BSPs in the application as filed.

Therefore, Applicant respectfully requests that the above rejection to claims 4, 5, 16 and 17 be withdrawn.

The Examiner also rejected claims 7 and 22 noting that the claims and the specification do not provide a standard for ascertaining the meaning of the term "Wireless Internet Facility (WIF)."

Applicant respectfully submits that WIFs are well described in the specification to enable one of ordinary skill in the art to ascertain a standard for the term WIF. Specifically, Applicant respectfully directs the Examiner's attention to the WIF depicted in Figs. 2, 4a and 5 of the drawings as originally filed, and to page 3, line 26 to page 4, line 7 of the specification as originally filed. Here, WIFs are clearly described as interfacing with the BSP to store mobile user profiles indicative of a firewall configuration corresponding to the mobile users. In addition, the stored profile information may indicate other transmission parameters to be applied to wireless communication with a particular mobile user.

Applicant believes one skilled in the art of wireless communication would be able to ascertain a standard term for the term WIF from the above-noted descriptions as well as other descriptions of WIFs in the application as filed. Therefore, Applicant respectfully requests that the rejection of claims 7 and 22 be withdrawn.

The Examiner also rejected claims 13 and 26 noting that the term "password scanning" is an indefinite term and is not defined by the claims and specification.

Applicant has amended claims 13 and 26 to change the words "password scanning" to "password cracking." Support for this change may be found in the specification at page 10, line 1 to page 11, line 11. Applicant believes these changes overcome the above rejection to claims 13 and 26, and respectfully requests that this rejection be withdrawn.

§ 103 Rejections

At paragraph 5 of the Office Action, claims 1-3, 8, 10-12, 14, 15, 18, 20, 23-25, 31 and 32 were rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent 5,758,088 to Bezaire et al. (hereinafter "Bezaire") in view of W. C. Yee, "Mobile Communications Design Fundamentals," Second Edition, John Wiley and Sons, 1993 (hereinafter "Yee").

The present invention relates to a technique for providing a firewall configuration corresponding to a mobile user in a wireless communications network. According to an aspect of the present invention, a firewall configuration is established for the mobile user located in an area of a particular wireless transceiver. When the mobile user is located in an area of a second wireless transceiver, the same firewall configuration is established at the second wireless transceiver.

Bezaire describes a technique for allowing a wireless device to receive select information via an information service. According to Bezaire, the wireless device is first registered with the information service. This registration entails providing information to the information service that indicates how to reach the wireless device. Optionally, rules for accepting messages on the wireless device may also be provided. See Bezaire, column 3, lines 29-49.

Further according to Bezaire, a message received by the information service is sent to the information service's mail server. The mail server applies any optionally defined rules to determine if the message is routed to the wireless device or filtered (i.e., not routed to the wireless device). If the message is routed to the wireless device, the message is sent through the information service's gateway. The gateway locates the information for the wireless device (specified when the wireless device was registered) and forwards the message along with the information to a wireless service provider. The wireless service provider uses the information to identify the wireless device and sends the message to the wireless device. See Bezaire, column 4, lines 20-39, see also, Figs. 1 and 2.

In section 5.5.2 of Yee, Yee describes a hand-off technique for mobile units in a cellular telephone system. According to Yee, as a mobile unit travels along a path that passes through different cells in the system, calls associated with the mobile unit are handed off from one cell to the next by a switching office. See Yee, section 5.5.2, pages 183-4.

Representative claim 1 recites:

> 1. A method of protecting a mobile wireless user via a firewall, the method comprising:
>
> defining a mobile user profile indicative of a firewall configuration corresponding to the mobile user;
>
> establishing the firewall configuration at ***a firewall application in a wireless transceiver*** corresponding to the current location of the mobile user, the wireless transceiver operable for wireless communication with the mobile user via a wireless access unit; and
>
> establishing the same firewall configuration at a second firewall application in a second wireless transceiver when the user is located in the area corresponding to the second transceiver.

Applicant respectfully submits that Bezaire taken either individually or in combination with Yee do not teach or suggest Applicant's claimed establishing the firewall configuration at ***a firewall application in a wireless transceiver***.

Yee is silent with regards to firewalls and firewall configurations. Bezaire fails to describe establishing a firewall in a transceiver. Rather, Bezaire describes filtering that occurs within an information service that does not contain a wireless transceiver.

For reasons set forth above, Applicant respectfully requests that the above § 103 rejection to claims 1-3, 8, 10-12, 14, 15, 18, 20, 23-25, 31 and 32 is prima facie deficient and thus should be withdrawn.

At paragraph 6 of the Office Action, claims 4, 5, 16, 17, 27 and 28 were rejected under 35 U.S.C. § 103 as being unpatentable over Bezaire and Yee, and in further view of the Nokia A032 brochure (hereinafter "Nokia").

Nokia describes an access point device that provides wireless access to local area networks (LANs) and the Internet. The access device acts as a wireless bridge between the wireless devices and, the LANs and Internet. In addition to providing bridging functions, the access device provides Wired Equivalent Privacy (WEP) encryption as well as a firewall capability that uses Network Address Translation (NAT) firewall technology. The WEP

encryption may be configured to allow certain wireless devices access to the wireless network while blocking other wireless access devices.

Applicant respectfully submits that Bezaire, Yee and Nokia, taken either singly or in combination do not teach or suggest Applicant's claimed ***establishing the same firewall configuration at a second firewall application in a second wireless transceiver when the user is located in the area corresponding to the second transceiver.***

As explained above, Bezaire and Yee do not teach or suggest ***a firewall application in a wireless transceiver***. Further, since Bezaire and Yee do not teach or suggest ***a firewall application in a wireless transceiver***, they fail to teach or suggest ***establishing a firewall configuration at a second firewall application in a second wireless transceiver when the user is located in the area corresponding to the second transceiver.*** Nokia teaches WEP encryption and a NAT firewall in a wireless access point that acts as a bridge between a LAN and the Internet, and wireless devices. However, Nokia does not teach establishing ***firewall configurations corresponding to a mobile user*** let alone ***establishing a firewall configuration in a second firewall application at a second wireless transceiver when the user is located in the area corresponding to the second transceiver***.

The Examiner seems to believe that the WEP encryption performed by the Nokia access point acts as a firewall. WEP encryption, as is well known in the art of encrypted wireless communication, provides for secure communication on a wireless link between the access point and a wireless device by encoding data with a code word or "key." WEP operates on the fact that both the access point and the wireless device know the same key. Thus, a wireless device that does not have the key is denied access to the network by the access point.

Nokia extends this concept by providing a means to specify personal keys for wireless devices (rather than having a single key that is used by all of the wireless devices). This enables a particular wireless device to be "locked out" merely by changing the wireless device's personal key. Although personal keys are used, the effect is the same as if a single key were used to gain access to the network, that is, if the correct personal key is supplied, access is granted to the network otherwise access to the network is denied.

Granting or denying access to a network is not a function typically performed by firewall applications. Firewall applications are typically designed to filter certain packets from a network

not grant or deny access to a network. See B.D. Chapman et al., "Building Internet Firewalls, 2nd Edition," O'Reilly, June 2000 in the art of record. Thus, the WEP encryption performed by the Nokia wireless access point is not a firewall and would not have the suggested firewall functions as urged by the Examiner.

As for NAT, NAT is a well known technique that may be used to map addresses from a private network domain (e.g., a private LAN) to addresses in a public network domain (e.g., the Internet). In the Nokia system, the NAT firewall converts addresses from the private network domain connected to the access point to an external address for use outside in the public network domain. See "Nokia A032 Wireless LAN Access Point Advanced User Guide," Nokia Internet Communications, Inc., Copyright 1999, 2000 submitted herewith and cited on an Information Disclosure Statement filed herewith. This way, users outside the firewall (i.e., outside the private domain) have no visibility of the addresses used in the private domain. Further, attempts to transfer packets that the use private network addresses from the public network domain side of the firewall to the private network domain are blocked by the firewall.

The NAT firewall described by Nokia does not use ***firewall configurations corresponding to a mobile user*** as is claimed by Applicant. Rather, the configuration used by NAT firewall described by Nokia is a general configuration that is used by all users and does not correspond to a particular user.

For reasons set forth above, Applicant respectfully requests that the above § 103 rejection to claims 4, 5, 16, 17, 27 and 28 be withdrawn.

At paragraph 7 of the Office Action, claims 5, 7, 21 and 22 were rejected under 35 U.S.C. § 103 as being unpatentable over Bezaire and Yee, and in further view of U.S. Patent No. 6,161,125 to Traversat et al (hereinafter "Traversat").

Traversat describes a data schema for representing and storing configuration and related information associated with clients in a client-server network in a system database. The schema comprises a client schema and a server schema. Data related to a client is stored in a client schema at the client. Configuration data for each of the clients is stored in the server schema at a network server. Configuration data is exchanged between the two schemas through a client/server protocol. Storing client configuration data in the server (which acts as a central repository for the client configuration information) enables the configuration information to be

updated at a single source and propagated to the clients. See Traversat, column 5, line 65 to column 6, line 31.

Applicant submits that Bezaire, Yee and Traversat taken either singly or in combination do not teach or suggest Applicant's claimed ***establishing the firewall configuration at a firewall application in a wireless transceiver***.

As discussed above, Bezaire and Yee do not teach or suggest ***a firewall application in a wireless transceiver***. Likewise, Traversat is silent with regards to firewalls and wireless transceivers let alone a firewall application in a wireless transceiver.

For reasons set forth above, Applicant respectfully requests that the above § 103 rejection to claims 5, 7, 21 and 22 be withdrawn.

At paragraph 8 of the Office Action, claims 9 and 19 were rejected under 35 U.S.C. § 103 as being unpatentable over Bezaire and Yee, and in further view of Newton's Telecom Dictionary, Eight Edition, Flatiron Publishing (hereinafter "Newton").

Newton describes an Electronic Serial Number (ESN) that is assigned to a cellular telephone. The ESN is used to authenticate the cellular telephone and grant it access to the cellular network.

Applicant submits that Bezaire, Yee and Newton taken either singly or in combination do not teach or suggest Applicant's claimed ***establishing the firewall configuration at a firewall application in a wireless transceiver***.

As discussed above, Bezaire and Yee do not teach or suggest ***a firewall application in a wireless transceiver***. Newton is silent with regards to firewalls and wireless transceivers let alone a firewall application at a wireless transceiver.

For reasons set forth above, Applicant respectfully requests that the above § 103 rejection to claims 9 and 19 be withdrawn.

At paragraph 9 of the Office Action, claims 13 and 26 were rejected under 35 U.S.C. § 103 as being unpatentable over Bezaire and Yee, and in further view of B.D. Chapman et al., "Building Internet Firewalls, 2nd Edition," O'Reilly, June 2000 (hereinafter "Chapman").

Chapman describes configuring a firewall with various parameters, such as source address, destination address, protocol, destination port, source port and acknowledge (ACK).

The parameters are used to qualify packets to determine if the packets should be allowed to pass through the firewall.

Applicant submits that Bezaire, Yee and Chapman taken either singly or in combination do not teach or suggest Applicant's claimed ***establishing the firewall configuration at a firewall application in a wireless transceiver***.

As discussed above, Bezaire and Yee do not teach or suggest ***a firewall application in a wireless transceiver***. Chapman is silent with regards to a firewall at a wireless transceiver.

For reasons set forth above, Applicant respectfully requests that the above § 103 rejection to claims 13 and 26 be withdrawn.

Information Disclosure Statement

An Information Disclosure Statement (IDS) is being filed concurrently herewith. Entry of the IDS is respectfully requested.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By Michael J. Badzinski

Michael J. Badzinski
Registration No. 51,425
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: 3/15/05